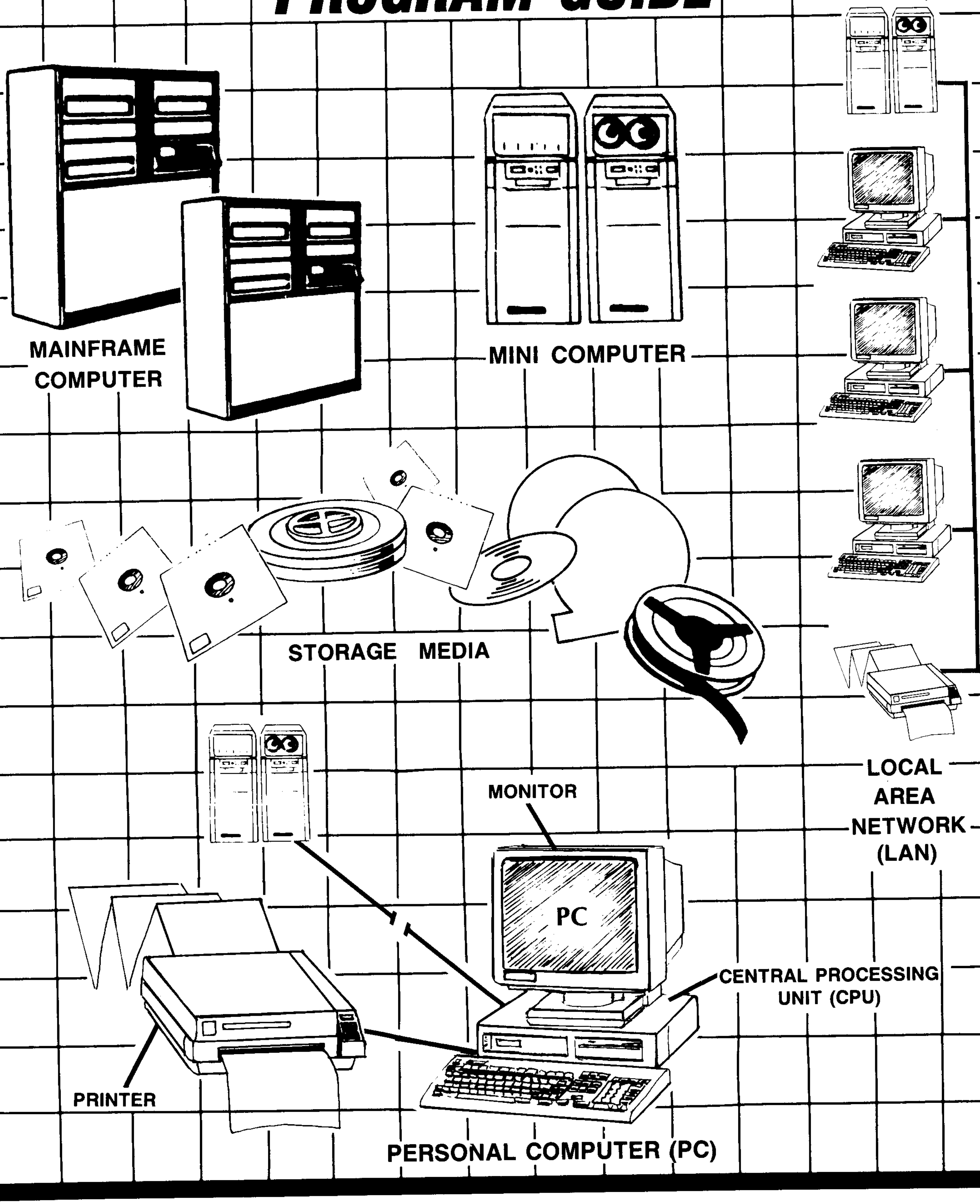
15 JULY 1991

AMC-P 380-4

INFORMATION SYSTEMS SECURITY PROGRAM GUIDE



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC PAMPHLET
No. 380-4

15 July 1991

Security

INFORMATION SYSTEMS SECURITY PROGRAM GUIDE

CONTENTS

Paragraph Page

SECURITY ACCREDITATION

APPENDIXES

PREFACE

This Information Systems Security Program Guide has been prepared for Information Systems Security Officers (ISSO) to assist in the implementation of an Information System Security (ISS) Program for your activity. The purpose of this guide is to ensure that automated information systems are properly accredited per AR 380-19, Information Systems Security, 1 August 1990.

For additional assistance or questions concerning accreditation of automated information systems, contact your Installation Systems Security Manager (ISSM).

SECURITY ACCREDITATION

1. Purpose: Research and interpretation of the applicable security regulations, publications, and other guidance involved in accreditation of automated resources can be time consuming and often confusing. This document is intended to assist activities in the development of the documentation and the implementation of an information systems security program. The basic directive is AR 380-19 which should be followed along with the AMC Supplement to AR 380-19 and examples contained in this guide. Due to the vast differences between accrediting a mainframe computer system that processes classified sensitive data, a small standalone computer performing basic administrative functions, or a series of computers linked together to form a local area network, the information contained herein is intended to serve as a guide for systems security accreditation.

2. Accreditation Documentation Classification: When an accreditation document is compiled, it describes in detail the vulnerabilities, risks, systems design, and the physical layout of the system. Because of this, consideration must be given to classifying the documentation at a level commensurate with the classification of threats and vulnerabilities identified. As a minimum, the documentation will be protected as "FOR OFFICIAL USE ONLY." (See AR 25-55, exemption categories 2 and 5.)

3. Accreditation Overview: Accreditation results from the process whereby information pertaining to the security of an Army Automated Information System (AIS) is collected, analyzed, and submitted for approval. Accreditation is the Designated Accreditation Authority's (D M) formal declaration that an AIS or network is approved to operate: in a particular security mode; with a minimal prescribed set of technical and nontechnical security safeguards; against a defined threat; in a properly secured area; in a given operational environment; under stated short and long-term goals; with stated interconnections to other AIS or networks; and at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The example in appendix A is directed toward microprocessors operating at the US-1 or US-2 level. Activities that have large systems or systems approved for classified processing may modify the example in appendix A to reflect those additional requirements identified in AR 380-19. The DAAs for systems operated by AMC personnel at the various levels of classification are identified in the AMC Supplement to AR 380-19. Additionally, several accreditation documents "using the generic approach" have been developed and approved by AMC Headquarters. These documents may be used as a basis for an accreditation document. They cover a variety of equipment configurations to include personal computer systems, multiuser systems, and word processing systems.

4. Appointments: For each AIS or group of AIS, there will be an Information System Security Officer (ISSO) appointed by the commander or manager of the activity operating the AIS. The same ISSO may be appointed for multiple AIS, particularly in the environment of small computers, local area networks, or small systems that are oriented toward the functional user as the operator. A list of the duties and responsibilities of the ISSO is provided

at appendix B. For each identified network, there will be a Network Security Officer (NSO) appointed who will implement the ISS program for the network within his or her purview. A list of the duties and responsibilities of the NSO is provided at appendix C. For each terminal or contiguous group of terminals not under the direct control of an ISSO or NSO, there will be a Terminal Area Security Officer (TASO) appointed. A list of duties and responsibilities of the TASO is provided at appendix D. The dut ies and responsibilities do not address every possible situation; therefore, when unusual conditions arise, contact the ISSM for additional guidance.

5. Physical Security: A balanced AIS security program must include a firm physical security foundation. The objectives are to safeguard personnel, prevent unauthorized access to equipment, facilities, material, media, and documents; safeguard against espionage, sabotage, damage, and theft; and reduce the exposure to threats which could cause a denial of service or unauthorized alteration of data. Physical security requirements are outlined in section IV, AR 380-19 (US-1 and US-2), appendix H, AR 380-5 (classified systems), and paragraph 2-8, AR 190-13 (mission essential or vulnerable areas). Data processing activities that are designated as mission essential/ vulnerable areas will be inspected every 18 months for classified sensitive systems and biennially for US-l and US-2 systems. These inspections will be conducted by physical security inspectors. All other systems will receive physical security support from the ISSM. This policy in not intended to reduce the importance of physical security in any way. The emphasis for the smaller systems (microcomputers and local area networks) is being directed toward adequate procedures and security awareness in lieu of costly construction measures. Each activity will be advised of the applicable policy during the accreditation process. In either case, the activity will be visited by the ISSM and physical security measures will be discussed and recommendations made to correct deficiencies.

6. Communications Security: Classified information will be transmitted only by secure means. Only NSA endorsed COMSEC products will be used to encrypt classified information. Protection of unclassified sensitive information during transmission will be consistent with the risk of disclosure, loss, misuse, alteration, destruction, or nonavailability. Protection requirements for US-l and US-2 systems are addressed in paragraph 4-3, AR 380-19.

7. Password Control: System passwords are critical to the security of a system. Their purpose is to identify users entering the system from a remote device. The ISSO oversees generation, issuance, and control of all passwords. All passwords should be generated by random generator software and must not be obtained from commonly used words or phrases. Knowledge of individual passwords will be limited to a minimum number of persons and passwords will not be shared. Passwords must be generated with, as a minimum, five character strings using the 35 alphabetic-numeric characters, or six character strings using only alphabetic characters. Password generation and control is outlined in paragraph 2-15, AR 380-19.

8. Privately-owned Computers: Per paragraph 5-4, AR 25-1, the use of employee-owned computers and software to process Government-related work at the work site is discouraged. However, the ISSM may approve or disapprove the use of employee-owned computers to perform work at the work site. If approved, a Memorandum of Agreement will be executed between the owner of the computer and the ISSM. If only unclassified, nonsensitive information will be processed on the computer, formal accreditation is not required.

9. Use of Laptop Computers for Off-site Processing: Laptop computers may be taken off the Government work site to process Army-related work. The accreditation must address all aspects of security and must specifically indicate the approved processing locations (in general terms such as work site, residence, temporary duty (TDY) location, etc.), any authorized connectivity (US-2 systems only), and the extent to which processing of unclassified sensitive data is permitted. More guidance may be found in paragraph 2-27f, AMC Supplement to AR 380-19.

10. Proprietary Software: Unless authorized by the copyright owner, the Army may only copy proprietary software for limited purposes (such as an archival copy) under the provisions of Section 117 of Title 17 United States Code. Unauthorized reproduction of copyrighted software violates Federal Law and policy established by AR 27-60.3

The proponent of this pamphlet is the U.S. Army Materiel Command. Users are invited to send comments and suggestions for improvement on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMCMI-C, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

WILLIAM B. McGRATH
Major General, USA
Chief of Staff

OFFICIAL:

THOMAS H. DOLAN
Chief, Operations and Support
Division

DISTRIBUTION: Initial Distr H (60) 1 ea HQ Acty/staff ofc
B LEAD (3,814)
AMXDO-OP (Stockroom) (100)
AMCMI-C (100)
AMXLX-LM (100)
Commander
- AMCCOM (AMSMC-SI) (75)
- AVSCOM (AMSAV-O) (20)
- CECOM (AMSEL-SI) (75)
- DESCOM (AMSDS-SI) (75)
- LABCOM (AMSLC-MI) (20)
- MICOM (AMSMI-SI-SE) (200)
- TACOM (AMSTA-SC) (20)
- TECOM (AMSTE-IS-I) (200)
- TROSCOM (AMSTR-Y) (20)

C, SSA (AMXPX) (25)
Dir, SIMA (AMXSI-TRC) (20)
AMCIM-OE (10)
AMCPE-SH (100)

APPENDIX A

REFERENCES

AR 25-1	The Army Information Resources Management Program, 18 November 1988
AR 25-55	The Department of the Army Freedom of Information Act Program, 10 January 1990
AR 27-60	Patents, Inventions, and Copyrights, 15 May 1974
AR 190-13	The Army Physical Security Program, 20 June 1985
AR 340-21	The Army Privacy Program, 5 July 1985
AR 380-5	The Department of the Army Information Security Program, 25 February 1988
AR 380-19	Information Systems Security, 1 August 1990
(C) AR 380-19-1	Control of Compromising Emanations (U), 4 September 1990
AMC Suppl 1	to AR 380-19, 4 January 1991
AMC Suppl 1	to AR 380-19-1, 4 January 1991
FIPS PUB 31	Federal Information Processing Standards Publication, Guidelines for Automatic Data Processing Physical Security and Risk Management
TB 18-108	Army Automation Continuity of Operations Plan, 1 November 1985

APPENDIX B

ACCREDITATION DOCUMENTATION EXAMPLE

CONTENTS

1. Basic System Information and Identification.

a. System Name or Title. List microcomputers by CPU and quantity. An example would be Zenith-248 (35ea).

b. System Category. Systems covered provide general automated information system (AIS) support.

c. Type Accreditation. This in an operational accreditation covering microcomputers throughout (list activity). It does not apply to computers operated by the Information Systems Command or to privately-owned computers.

d. System Status. These systems are operational.

e. System Overview. These systems are used primarily for office administration. They may also be used for specific purposes such as data base administration, inventory management, financial management, software development, testing programs, computer-aided instruction, and receiving or transmitting data to other systems. These systems may process any variety of information, provided the protection level does not exceed US-l or US-2. If laptop computers are to be taken off the work site; indicate the approved processing locations (in general terms such as "residence," "TDY locations," and so forth), any authorized connectivity, and the extent to which processing of unclassified-sensitive data is permitted.

f. System Environment and Special Considerations. Users must protect the systems from misuse, abuse, unauthorized access, and theft. Users are also responsible for properly protecting their data. Describe location(s) of systems and list special considerations.

g. Information System Security Officer Appointment. As a minimum there will be an ISSO and alternate ISSO appointed for each activity. Additional appointments such as for each building, division, or branch within an activity is optional. Appointment orders will be attached to this accreditation as an enclosure. See Tab A for sample format.

h. System Identification. Paragraph la above describes systems covered by this accreditation. Each activity will attach a Facility Security Profile (FSP) (listing specific equipment serial numbers and all installed software) to this accreditation. The FSP must indicate the processing level (US-l or US-2). See Tab B for sample of format.

i. Near and Long-Term Goals. Users may determine what applications are performed and will ensure all processing is accomplished in the best interest of the Government. These systems will be used only for official Government business. Systems may be used to access other unclassified sensitive systems provided the security and connection requirements of the host system are met. (See appendix C, (C-l), AR 380-19 for large systems.)

2. Sensitivity, Protection Requirements, Security Mode, and Minimum Trusted Class.

a. Sensitivity Designation--

(1) US-l: Unclassified information requiring protection from foreign intelligence services to ensure confidentiality and which involves: intelligence activities, cryptologic activities related to national security; command and control of forces; is contained in systems that are an integral part of a weapon or weapon systems; or is contained in systems that are critical to the direct fulfillment of military or intelligence missions. US-l information is exempt from the Computer Security Act of 1987.

(2) US-2: Unclassified information requiring protection primarily to ensure its availability or integrity. Included is information requiring protection from foreign intelligence services or other unauthorized personnel to ensure confidentiality. Such information may deal with logistics, medical, personnel management, Privacy Act data, contractual data, and FOR OFFICIAL USE ONLY information. Other information that is sensitive in nature, such as certain categories of financial data, that does not require protection to ensure its confidentiality, is also included. The Computer Security Act applies to US-2 data.

b. Protection Requirements. These systems require protection to ensure integrity, availability, and confidentiality. Of primary concern to US-l users is confidentiality. The primary concern of US-2 users is data availability. Paragraph 4 details protection requirements for both levels.

c. Security Mode of Operation. Identify mode as either Dedicated or Systems High.

d. Minimum Trusted Class. Although not formally rated, the security features should strive to meet the Cl Class as defined in DOD 5200.28-STD. This means users are accountable for their actions on the systems. Access control policy will be addressed in the SOP. Users will participate in periodic computer security training. Training will identify all threats, vulnerabilities, and risks associated with the systems. It will also discuss media handling and storage, access controls, and emergency plans.

3. Risk Management Review.

a. Unauthorized disclosure of data.

(1) Risk. Personnel use their computers to create correspondence, reports, etc., which may require protection under the Privacy Act of 1974.

(2) Risk Assessment. The risk from this threat is low since all Government employees undergo initial screening before employment. All users, though they may not have a security clearance, will have a minimum of a National Agency Check or an Entrance National Agency Check before permanent employment with the Government. Additionally, users are subject to ongoing review by supervisors and AIS security personnel. This risk is acceptable.

b. Unauthorized manipulation of data.

(1) Risk. This threat comes from both authorized users (either intentional or through errors) and from hostile agents.

(2) Risk Assessment. The risk from this threat is low because of the limited access to other users' data. Users are instructed to protect their data from those individuals who do not have a need to know. Additionally, the standing operating procedures (SOP) will instruct users to store backup copies of their data on removable media, further restricting unauthorized access. This risk is acceptable.

c. Unauthorized system use.

(1) Risk. Unauthorized users may gain access to internally-stored data.

(2) Risk Assessment. The risk from this threat is low if software is stored on removable media, and moderate when stored on fixed media. Procedural controls must ensure only authorized users may use the systems. This risk is acceptable.

d. Denial of service.

(1) Risk. If a computer fails due to hardware, software, or power problems, operations will be degraded. This threat could come from natural or manmade disasters or hostile action.

(2) Risk Assessment. The risk from this threat is moderate. All systems are susceptible to this threat because of the variety of possible causes. USAMC activities will have maintenance contracts in place to ensure timely correction of problems caused by hardware, software, or communications failure. Users will be trained in emergency procedures in case of a natural or manmade disaster. Procedural controls must be in place to restrict any manipulation by hostile agents. This risk is acceptable.

e. Electrical damage.

(1) Risk. Power surges can damage systems and render internally stored information permanently inaccessible. Static electricity, caused by low humidity and/or lack of grounding devices, can also damage these systems.

(2) Risk Assessment. The risk from this threat is low. The disruption of processing is usually limited to a few hours. This delay is acceptable. To reduce the possibility of disruption, all systems will be connected to a surge protector and grounding devices to bleed away static electricity.

Antistatic sprays, carpets, pads, or humidifiers can also help. Instruct personnel to discharge any built-up static charge by touching a grounded object, such as a metal desk or doorknob. This risk is acceptable.

f. Air pollution.

(1) Risk. The general cleanliness of the processing area affects contaminant levels. Disk drives are especially sensitive to airborne particles.

(2) Risk Assessment. The risk from this threat is moderate. Though it is not generally necessary to install special purpose air purifiers in

processing areas, eliminating contaminants such as smoke, dust, and tobacco ash helps protect systems. Keep airborne contaminants as far away as possible from these systems. The SOP will address this problem and instruct users on backup procedures. This risk is acceptable.

g. Heat and humidity.

(1) Risk. Temperatures over 90 degrees Fahrenheit can cause the systems to fail. Excess humidity can cause condensation on circuit boards or magnetic media. Fires or simple lack of air conditioning can cause these problems.

(2) Risk Assessment. The risk from these threats is low. Air conditioning solves most of the problem. This risk is acceptable.

h. Unauthorized physical access.

(1) Risk. These systems may be in areas where different levels of processing are permitted. They may also be in open bays, high traffic areas, and remote areas with little traffic. Physical security varies widely, depending on the organization's mission.

(2) Risk Assessment. The risk from this threat is low. Most users are in buildings where access is controlled by personnel occupying the buildings. Those individuals whose equipment is in uncontrolled areas must be instructed on procedures to follow when confronted by unfamiliar personnel. This risk is acceptable.

i. Water damage.

(1) Risk. Some systems may be located near water pipes and sprinkler systems.

(2) Risk Assessment. The risk from broken pipes or malfunctioning sprinklers is low. Generally, buildings are located on relatively high ground and are not located in any flood plain area. Excess equipment should not be stored in such a manner to make it vulnerable to flood damage. During periods of high flood risk, equipment can be moved to upper floors, placed on top of tall furniture, or covered by waterproof material. These risks are acceptable.

j. Natural disasters.

(1) Risk. Fire and excess heat can cause damage very quickly. Floods (because of contamination with dirt, oil, or chemicals) can completely destroy equipment. Hurricanes and tornadoes are also potential threats. Earthquakes are a threat for two reasons. First, they can cause structural damage or collapse of the facility housing the equipment. Second are the more widespread effects on the community (disruption of transportation, food supplies, and other vital services) which can result in users not being able to report for work.

(2) Risk Assessment. The risk from this threat is moderate. Systems must be located as far as possible from open flames or other heat sources. In

addition, users will be familiar with local procedures in case of fire. Fire protection equipment will be installed per local fire codes. Most facilities provide adequate storm protection. The probable result of storms is disruption of service. The threat of earthquake is based upon the Seismic Risk Map of the United States as shown in FIPS PUB 31. These risks are acceptable.

k. Other environmental considerations.

(1) Risk. Food and drink spillage can damage computers and magnetic media.

(2) Risk Assessment. The risk from this threat largely depends on the individual user. It is highly recommended that users not be allowed to eat, drink, or smoke near computer equipment. The SOP will discuss the hazards of eating, drinking, and smoking near computer equipment. This risk is acceptable.

4. Implementation of Controls and Countermeasures.

a. Physical Security. Adequate physical security controls should be in place through the use of barriers, procedures (outlined in the SOP) and access controls which reduce the probability of unauthorized access to an acceptable level. Physical security barriers include restricted area signs, end of day security checks, door and window locks, access rosters, location of terminals in controlled access areas, and security of restricted areas during nonduty hours.

b. Personnel Security. All users should have completed a favorable National Agency Check or an Entrance National Agency Check. Supervisors are responsible for maintaining control over their personnel. All users will receive periodic briefings on computer security policy and procedures.

c. Communications Security. These systems may be used to access other computers. The host system dictates security procedures in such cases. Connection to unclassified sensitive systems may be made from off site locations. US-1 systems require protection in transmission unless waived in writing by the local accreditation authority on a case-by-case basis. Use techniques approved by the National Security Agency or National Institute of Standards and Technology.

d. Hardware Security. This type of security is usually not present in microcomputers. Procedural security can counter hardware vulnerabilities.

e. Software Security. Users will run only software specifically developed or approved for use, or which has been purchased or leased by authorized U.S. Government representatives. Use of public domain, shareware, or other privately-owned software, regardless of source, is prohibited unless approved by the activity ISSO. The FSP will list the software used on each system (including operating system) by name and version number. Control all software to prevent unauthorized changes. Enforce copyright laws. Do not make additional copies (other than backup copies) unless permitted by the license agreement.

f. Procedural Security. All activities will have an Information Systems Security Officer (ISSO) appointed in writing. Appoint Network Security Officers and Terminal Area Security Officers as necessary. Procedural security features that ensure the protection of data being processed include -

(1) Marking and protection of all media and output covered by the Privacy Act of 1974, or which qualifies for "FOR OFFICIAL USE ONLY" protection.

(2) Clear delineation of ISSO duties.

(3) Periodic user training .

(4) Use of SOP.

(5) Periodic risk management review.

g. Continuity of Operations Plan. Perform backups periodically (at least once a week) and store them separately from the original media. In case of inoperability, a user should be able to use another system in the general area. If another like system is not available, the user may revert to manual methods to complete his tasks. NOTE: Continuity of Operations Plan for large systems is addressed in TB 18-108.

5. Certification Test. Not applicable for microcomputers. Activities which have large computer systems must complete a certification test under a certification plan to determine whether the system adequately meets its prescribed security requirements. Certification test requirements are addressed in paragraph 3-4, AR 380-19.

6. Facility Information. The Facility Security Profile (FSP) found at Tab B describes all hardware and software. Additional requirements for large computer systems are addressed in appendix C, (C-6), AR 380-19.

7. Network Considerations. For systems being accredited as a separate AIS in the interconnected Accredited AIS (IAA) view, indicate the network DAA (if identifiable), and describe the conditions under which connection to the IAA has been approved. For Single Trusted System (STS) view networks, this section should address the network's capability to provide communications integrity, protection against denial of service, and compromise protection. (See paragraph 2-23c, AR 380-19.)

8. Attachments.

TAB A - ISSO appointment orders (NSO and TASO orders, if required)

TAB B - Facility Security Profile

TAB C - Local AIS SOP

TAB A

APPOINTMENT ORDERS EXAMPLE

(OFFICE SYMBOL) (380-19a)   DATE

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Duty Appointment

1. The following named individual is appointed as Information System Security Officer (ISSO) for (ACTIVITY):

(NAME)   (GRADE)

2. Authority: Paragraph 1-6d(3), AR 380-19.

3. Period: Indefinite.

4. Special Instructions: None

5. This appointment supersedes all previous appointment orders.

SIGNATURE BLOCK OF ACTIVITY HEAD

TAB B

FACILITY SECURITY PROFILE EXAMPLE

1. Indicate the organizational name and office symbol.

2. Identify the ISSO's name and telephone number.

3. Identify the building and room number where the equipment is located.

4. Indicate sensitivity level of processing (e.g., unclassified-sensitive 2).

5. List equipment type, manufacturer, model number, and serial number.

6. Identify all operations and applications software; to include software that is government-owned or leased, shareware, freeware, and software obtained through the public domain.

TAB C

STANDING OPERATING PROCEDURE EXAMPLE

1. Purpose. The purpose of this Standing Operating Procedure (SOP) is--

a. To establish policies, procedures and doctrine pertaining to microprocessors and USI or US2 data contained therein.

b. To provide general and technical information and guidance for the daily operation of microprocessors and the handling of US1 or US2 data.

2. General. The (list activity) will utilize these microprocessors to process general, as well as, specific data relating to typical (list activity) functions and missions. At no time will any of this data consist of classified information.

3. Applicability. This SOP is applicable to all (list activity) personnel. Should a conflict arise between this SOP and AR 380-19, regulatory guidance provided in AR 380-19 will always be given priority.

4. Operational Control. Operational control will be at the following hierarchical ranking:

a. Directorate level. The Directorate Information Systems Security Officer (ISSO) maintains operational control functioning on behalf of the Director, (list activity). Duties and responsibilities are outlined in paragraph 1-6d(3a-m), AR 380-19.

b. Division level (if appropriate). The Terminal Area Security Officers (TASOs) maintain operational control for their division on a routine, daily basis functioning on behalf of the Division Chief.

5. Procedures.

a. All computer users will be aware of all Directorate AIS security procedures and will report to their supervisor any suspected abuse or violation of these procedures.

b. The system will always be "brought up" by first plugging in the station protector into a proper wall outlet. Next flip the "on" switch which is a part of the station protector. This will "bring up" the entire system and any attached peripherals. If any problem is encountered during this process, notify the ISSO immediately.

c. Access to microcomputers will be limited to designated user(s) within a particular division, or further restricted as directed by each division chief. An official list of any and all personnel authorized access to microprocessors will be posted in plain view of, or attached to, the monitor of each machine.

d. No user will make any unauthorized copy of a data file or files containing Privacy Act information, and/or proprietary software files.

e. No user will knowingly allow Privacy Act information to be compromised.

f. Users will take care to arrange the physical layout of work stations and monitors as to prevent unauthorized viewing by personnel visiting the (list activity) during duty hours. Personnel not assigned to (list activity) should not be allowed to wander freely through any buildings. Division Chiefs will establish policies to ensure that visitor access is controlled during the noon hour and at other times when the majority of assigned personnel are temporarily absent.

g. At the end of each user session, the user will power down and unplug the system if no further system usage is anticipated.

6. Physical Security. Due to the relatively small size of microcomputers and their portability, they are highly vulnerable to theft. It is imperative that these systems have adequate physical security when office areas are unoccupied, especially during nonduty hours. A good key control policy must be in place at all times to ensure maximum protection is provided these systems.

7. Maintenance.

a. Maintenance: The (list activity) maintenance coordinator (name of individual) and/or ISSO will be notified immediately if there are any problems with hardware or software.

(1) Hardware. All hardware problems will be repaired by Director of Information Management technicians. The Information Center (list point of contact (POC) and phone number) will be contacted for assistance.

(2) Software. Diskettes, diskette files, paper, ribbon, ink, etc., will be procured through the activities supply and services account.

(a) Software Diskettes. These are precision recording media and can be easily damaged. The following procedures on diskette use must be enforced:

1. Keep diskettes in sleeves or holders when not in use.

2. Keep diskettes away from magnetic fields.

3. Do not touch the exposed areas on the diskettes.

4. Keep away from sun, extreme heat and cold.

5. Do not write on diskette or label using a hard pen/pencil.

6. Store vertically to avoid pressure to the sides.

7. Do not expose to dust, smoke, or ashes.

8. Protect from theft; secure properly.

(b) Backup Diskettes. A backup copy is recommended from each production program and data file diskette. If this diskette has to be used, another backup should be created before use. The paper copies and backup diskettes will be maintained per the Modern Army Recordkeeping System (MARKS) and stored in a different location than the originals in case of fire or other disaster under the Continuity of Operations Plan.

8. Training. Several options are available for AIS training. An initial security training and awareness briefing for AIS managers and users will be conducted by the ISSO. Training outside (list activity) is conducted periodically on a wide variety of AIS subjects and will be available to personnel who are performing ISSO functions.

9. Security. A balanced AIS security program must include a firm physical security foundation. The objectives are to--

a. Safeguard personnel.

b. Prevent unauthorized access to equipment, facilities, material, and documents.

c. Safeguard against espionage, sabotage, damage, and theft.

d. Reduce the exposure to threats which could result in a disruption or denial of service.

10. Privately-owned Computers. Per paragraph 5-4, AR 25-1, the use of employee-owned computers and software to process Government-related work at the work site is discouraged. However, the activity head, as appropriate, may approve or disapprove the use of employee-owned computers to perform work at the work site after technical review and approval by the ISSM. If approved, the system will be accredited under a separate accreditation plan.

11. Use of Laptop Computers for Off-site Processing. Laptop computers may be taken off the Government work site to process Army-related work. The accreditation must address all aspects of security and must specifically indicate the approved processing locations (in general terms such as work site, residence, TDY location, and so forth), any authorized connectivity (US-2 systems only), and the extent to which processing of unclassified-sensitive data is permitted.

12. Proprietary Software. Unless authorized by the copyright owner, the Army may only copy proprietary software for limited purposes (such as an archival copy) under the provisions of Section 117 of Title 17, United States Code. Unauthorized reproduction of copyrighted software violates Federal Law and policy established by AR 27-60.

13. Environmental Hazards. Smoke, dust, and other contaminants can easily damage many components of a typical small computer. Measures to reduce environmental hazards include: keeping areas in which computers are located clean; not permitting eating, drinking, or smoking in the immediate area of the computers; and keeping the computers away from open windows, direct sunlight, radiators, and heating vents.

APPENDIX C

DUTIES AND RESPONSIBILITIES OF THE ISSO
(Paragraph 1-6d(3), AR 380-19)

For each AIS or group of AIS, there will be an ISSO appointed by the commander or manager of the activity operating the AIS. The ISSO will --

a. Ensure systems are operated and maintained per AR 380-19.

b. Ensure users have the required personnel security clearance, authorizations, and need-to-know. Include all users, operators, and managers associated with the system in the security training and awareness program.

c. Conduct threat and vulnerability assessments to enable the commander or manager to properly assess risks and determine effective measures to minimize such risks.

d. Prepare, distribute, and maintain plans, instructions, guidance, and SOP concerning the security of system operations.

e. Report immediately to the facility manager and ISSM any attempt to gain unauthorized access to information, any system failure, or suspected defect which could lead to unauthorized disclosure.

f. Review and evaluate the security impact of system changes, including interfaces with other telecommunications and automated information systems (TAIS).

g. Report security incidents and technical vulnerabilities to the ISSM per this regulation and AR 380-5.

h. Prepare or oversee the preparation of the accreditation documentation and initiate reaccreditation when changes affecting security have occurred.

i. Establish a system for issuing, protecting, and changing system passwords.

j. Oversee the review of system audit trails and investigate discrepancies thoroughly.

k. Maintain access control records and establish an access control policy in which only authorized personnel can gain access to the system.

l. Ensure that a TASO is appointed for each terminal or contiguous group of terminals that are not under the direct control of the ISSO.

APPENDIX D

DUTIES AND RESPONSIBILITIES OF THE NSO
(Paragraph 1-6d(4), AR 380-19)

For each identified network, there will be an NSO appointed who will implement the ISS program for the networks within his or her purview. The NSO will --

a. Ensure that security procedures and protocols governing network operations are developed and issued.

b. Ensure that measures and procedures used at network nodes fully support the security integrity of the network and comply with applicable directives.

c. Establish a procedure to control access and connectivity to the network.

d. Prepare, disseminate, and maintain plans, instructions, guidance, and SOPs concerning security of the network.

e. Conduct reviews of threats to, and vulnerabilities in the network.

f. Report immediately to the manager of the network any system failure which could lead to unauthorized disclosure or attempts to gain unauthorized access to sensitive defense information.

g. Review and evaluate the security impact of changes to the network, including interface with other networks.

h. Coordinate and monitor periodic security indoctrination and training sessions for assigned personnel.

i. Ensure that audit trails and other system management reports are reviewed and used for internal security audits or testing.

APPENDIX E

DUTIES AND RESPONSIBILITIES OF THE TASO
(Paragraph 1-6d(5), AR 380-19)

1. For each terminal or contiguous group of terminals not under the direct control of an ISSO or NSO, there will be a TASO appointed. The TASO will perform the following duties as required by the ISSO or NSO:

a. Issue written instructions specifying security requirements and operating procedures.

b. Establish each terminal user's identity, need-to-know, level of clearance, and access authorization commensurate with data available from that terminal.

c. Establish procedures to restrict entry of unauthorized transactions or data.

d. Monitor local compliance with security procedures.

e. Assist the host system ISSO in providing system security.

f. Report actual or suspected security violations or incidents to the host system ISSO.

2. Responsibilities of a Terminal User:

a. Will adhere to the security requirements for use and protection of remote terminals, individual passwords, site identification codes and data transmitted to and from the host system.

b. Will handle all input/output commensurate with the terminal's level of sensitivity.

c. Will sign-off the terminal when the operation is complete.

d. Will not disclose or transfer system entry features (i.e., phone numbers, site identifications (IDs), user IDs, personal passwords, perishable passwords, and data base passwords) from one user to another.

e. Will not attempt to transmit and/or extract classified data via an unsecured remote device.

f. Will not create or use files which contain data elements not required for processing official requirements.

g. Will report terminal problems to the TASO for resolution.

h. Will obtain access approval from TASO prior to using a terminal other than the terminal(s) authorized for use.

3. TASO Checklist:

a. Is the distribution of phone numbers, site IDs, and passwords to authorized users properly controlled?

b. Does the TASO conduct periodic training in regard to the existing regulations and procedures governing the proper usage of the terminal and sign on procedure?

c. Does the TASO have a listing of personnel who are authorized to access the terminal(s) and what type outputs they may obtain?

d. Are the terminal(s) positioned in such a manner to prevent viewing of entry data by unauthorized personnel?

e. Is there a procedure for reporting terminal problems?

f. Is there a procedure for reporting security violations?

g. Is there a roster of authorized users posted?

h. Is there a procedure for the user to follow when extracting or transmitting classified data on the terminal?

i. Does the user know his/her TASO and whom to contact when problems occur?

j. Are users safeguarding their password and other system entry features?

k. Are terminals disconnected from the host if they are left unattended for a specific period of time?

l. Are removable storage media properly stored?

m. Does the TASO periodically check the terminal output products to ensure valid use of the system?

n. Do the users comply with proper sign on/off procedures?

o. Are instructions specifying security requirements and operating procedures issued for each terminal?

NOTE: Additional items can be added to this list to meet the specific needs of your terminal area.

APPENDIX F

SECURITY PROCEDURES FOR DATA DISKETTES

1. Diskettes containing sensitive Privacy Act data will be marked "FOR OFFICIAL USE ONLY - Privacy Act Data." Both the label on the diskette and its protective jacket will be appropriately marked.

2. Diskettes containing classified data will be handled and marked per AR 380-5. Both the label on the diskette and its protective jacket will be appropriately marked.

3. Diskettes will be kept in their protective jacket and stored in the appropriate container according to the sensitivity of the data stored on them to prevent unauthorized access, damage, modification, or destruction.

4. If diskettes become defective and are to be destroyed, the media should also be reformatted, reinitialized, or degaussed before being shredded or placed in a container for destruction.

5. Note that "deleting" or "killing" a file does not remove the data contained in that file from the diskette. Therefore, diskettes containing sensitive information must be reformatted, reinitialized, or degaussed prior to reuse.

6. Backup copies of sensitive data should always be maintained and stored away from work areas. Backup copies of sensitive data must be protected in the same manner as the original data.

7. Diskettes will not be removed from the organization without written approval from the ISSO.

8. On multiuser systems, each user should maintain his/her own diskettes. Those data files maintained on the hard disk should be write-protected to avoid damage or destruction by other users.

9. As an item of government property, diskettes are subject to inspection/examination for the presence of unauthorized data or software.

10. Diskettes and the files contained therein should be marked and labeled per the Modern Army Record Keeping System.

APPENDIX G

PROTECTION PROCEDURES FOR DATA DISKETTES

Diskettes must be protected when removed from their protective jackets. The following actions must be avoided in order to properly protect diskettes:

a. Do not place diskettes on terminals, in books, or under equipment. Do not toss a diskette loosely in a drawer.

b. Avoid placing diskettes near any magnetic source such as telephones, radios, tape recorders, or speakers of any kind.

c. Diskettes scratch easily. Do not touch exposed areas or try to wipe them clean.

d. Keep diskettes out of direct sunlight and away from extreme heat or cold.

e. Do not write directly on a diskette with a ball point pen, lead pencil, or other hard writing instrument. Instead, use a felt tip pen and a label.

f. Diskettes should be stored vertically in their jackets in either diskette storage trays or boxes to avoid pressure to the sides.

g. Diskettes containing sensitive information should not be left unattended in personnel computers or word processors.

h. Diskettes will not be exposed to cigarette smoke, ashes, or liquids of any kind.